AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒



AO386-B
DEFENDANT'S EXHIBIT
CASE NO. 25-cr-6-jdp
EXHIBIT NO. A

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
White 2014 Forest River Grey Wolf travel trailer bearing Illinois license plate 800938RT; Blue 2000 Dodge Ram 1500 bearing Wisconsin license plate TF4493, Whitewater Self Storage Unit #114, W8290 Sunrise Ln, Whitewater, WI, and the person of James Morgan (formerly Karactus Blome) (DOB 5/X/1993); all more fully described in Attachment A

Case No. 23-M-532 (SCD)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
*(identify the person or describe the property to be searched and give its location)*:
see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:
See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before 1-2-24 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Stephen C. Dries.
*(United States Magistrate Judge)*

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 12-19-23. 8:40 am

Stephen C. Dri
*Judge's signature*

City and state: Milwaukee, WI

U.S. Magistrate Stephen C. Dries
*Printed name and title*

| **Return** | | |
|---|---|---|
| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
| Inventory made in the presence of : | | |
| Inventory of the property taken and name(s) of any person(s) seized: | | |

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

## ATTACHMENT A

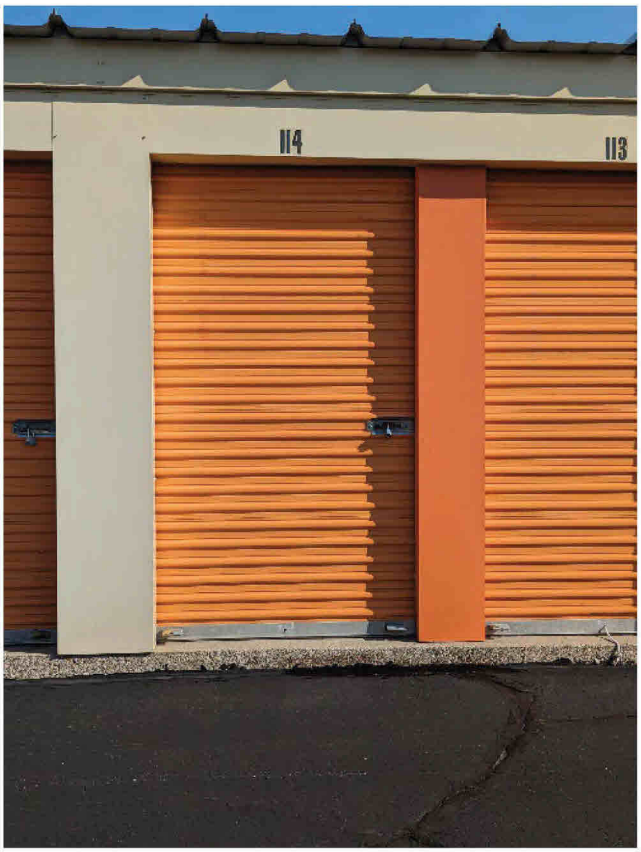
### Property and Person to Be Searched

The property and person to be searched are:

– White 2014 Forest River Grey Wolf travel trailer bearing Illinois license plate 800938RT, VIN: 4X4TCKB28EK023093, that is the residence of James Morgan (formerly known as Karactus Blome).


– Blue 2000 Dodge Ram 1500 bearing Wisconsin license plate TF4493, VIN 1B7HF16Z0YS539750.


– Whitewater Self Storage Unit #114, W8290 Sunrise Ln, Whitewater, Wisconsin. The storage unit is a locked unit with the unit number located directly above the door.




– The person of James Morgan (formerly Karactus Blome) (DOB: 5/9/1993, including all items in his possession, on his person, or in areas within his immediate control.

# ATTACHMENT B

## Particular Things to be Seized

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 842(p) (teaching or demonstrating the making or use of weapons of mass destruction), 18 U.S.C. § 229(a) (develop, produce, possess or conspire to use a chemical weapon), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 875(c) (communication of threats), and 26 U.S.C. § 5861 (receive, possess, or make firearm or destructive device in violation of the National Firearms Act) (the "subject offenses") involving James Morgan (aka Karactus Blome) and occurring after August 1, 2019, including:

1. Records and information relating to the subject offenses described above, including chemical weapons, chemical weapon precursor chemicals, weapons of mass destruction, and destructive devices;

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the subject offenses;

3. Preparatory steps taken in furtherance of those offenses;

4. Evidence of motive, intent, or knowledge of those offenses;

5. Computers or storage media that constitute fruits, contraband, evidence, or instrumentalities of the crimes described in the warrant.

6. For any storage medium whose seizure is otherwise authorized by this warrant, and any storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "computer"):

a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

h. evidence of the times the computer was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the computer;

j. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

k. records of or information about Internet Protocol addresses used by the computer;

l. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, cell phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files, web cache information, and handwritten notes), regarding the subject offenses.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. During the execution of the search of the premises described in Attachment A, law enforcement personnel are also specifically authorized to compel James Morgan (formerly known as Karactus Blome) to provide biometric features, including pressing fingers (including thumbs) against and or putting a face before a sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the premises, and
b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the subject offenses as described in the search warrant affidavit and warrant attachments

for the purpose of attempting to unlock the device's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to request Morgan state or otherwise provide the passcode or password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique fingers or other physical features) that may be used to unlock or access the devices.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

White 2014 Forest River Grey Wolf travel trailer bearing Illinois license plate 800938RT; Blue 2000 Dodge Ram 1500 bearing Wisconsin license plate TF4493, Whitewater Self Storage Unit #114, W8290 Sunrise Ln, Whitewater, WI, and the person of James Morgan (formerly Karactus Blome) (DOB 5/X/1993); all more fully described in Attachment A

Case No. 23-M-532 (SCD)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

see Attachment A

located in the Eastern District of WI, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 842(p) | teaching or demonstrating the making or use of weapons of mass destruction |
| 18 U.S.C. § 229(a) | develop, produce, possess, or conspire to use chemical weapon |
| 26 U.S.C. § 5861 | receive, possess, or make firearm or destructive device |

The application is based on these facts:

see affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

JUSTIN MOSIMAN Digitally signed by JUSTIN MOSIMAN Date: 2023.12.18 11:51:08 -06'00'

*Applicant's signature*

FBI SA Justin Mosiman

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 12-19-23

Stephen C. Dries

*Judge's signature*

City and state: Milwaukee, WI

U.S. Magistrate Judge Stephen Dries

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Justin Mosiman, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the residence, vehicles, and storage unit of James Morgan, as described in Attachment A, and the person of Morgan, including any property and belongings in his possession or in areas within his immediate control, all as further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2019. I have also been a Special Agent Bomb Technician since February 2021. I am currently assigned to the Joint Terrorism Task Force in Milwaukee, where I investigate violations of federal law. I have investigated and assisted in the investigation of matters involving violations of federal law related to counterterrorism and domestic terrorism, including the service of search and arrest warrants. Prior to my employment with the FBI, I served in the U.S. Navy for six years as an Explosive Ordnance Disposal Technician and provided contract support as an Explosive Ordnance Disposal Subject Matter Expert to the Department of Defense and Department of Energy for twelve years collectively.

3. The facts in this affidavit are known to me through my personal knowledge, training, experience, and through information provided to me by other law enforcement officers in the course of their official duties, whom I consider to be truthful and reliable.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 842(p) (teaching or demonstrating the making or use of weapons of mass destruction), 18 U.S.C. § 229(a) (develop, produce, possess, or conspire to

use chemical weapon), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 875(c) (communication of threats), and 26 U.S.C. § 5861 (receive, possess, or make firearm or destructive device in violation of the National Firearms Act) (together, the "subject offenses") have been committed by James Morgan (formerly known as Karactus Blome).[1] There is probable cause to search the locations described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

## JURISDICTION

6. This Court has authority to issue a warrant to search for and seize property located within the Eastern District of Wisconsin, property located within the Eastern District of Wisconsin that might be moved outside the district before the warrant is executed, and property within or outside the Eastern District of Wisconsin in a domestic terrorism investigation where related activities may have occurred. Fed. R. Crim. P. 41(b)(1), (2), and (3).

## PROBABLE CAUSE

7. Blome, age 30, lived with his mother and stepfather in Wheeling, Illinois, until August 2019, when he moved into his father's residence in Janesville, Wisconsin.

8. During an interview in September 2019, a family member provided information that Blome was extremely racist and prejudicial toward all people of color, creeds, and ethnicities that are not Blome's own. The family member also stated that Blome had an extreme disdain for law enforcement, all forms of government, and all perceived authority. Since childhood, Blome had difficulties with physical and verbal altercations due to extreme anger management issues. Later, in

[1] In December 2022, Blome petitioned for and was granted an order in Walworth County, Wisconsin, to change his name to James Morgan. In this affidavit, he will be referred to by Blome or Morgan, depending on the timing.

October 2019, the family member provided an additional general concern that Blome's anti-government behavior and rhetoric was accelerating after Blome moved to Janesville with his father.

9. The University of Wisconsin, Whitewater (UW-Whitewater) provided records showing that Blome enrolled as an undergraduate in the College of Letters and Sciences in the fall of 2021. In fall 2022, he was taking Chemistry II. As of November 15, 2023, he was not enrolled in classes, had a 3.5 grade point average, and had completed 68 credit hours toward an undergraduate degree in the letters and sciences program.

10. In June 2022, after his father's death, Blome moved from Janesville to an apartment in the Fox Meadow Apartments located at 291 N Fraternity Lane, Whitewater, Wisconsin.

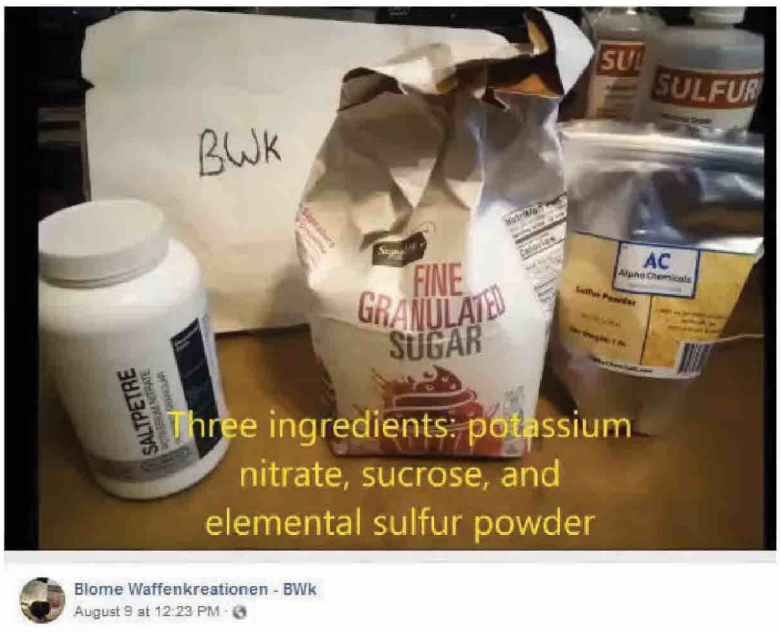
11. Beginning in November 2019, Morgan worked part-time at Generac Power Systems in Whitewater as a painter and assembler on an assembly line for commercial and residential backup power generator engines. Blome lost his job at Generac in December 2022 due to a large-scale termination of employees, and moved into a travel trailer in the summer of 2023. He currently is working at a fast-food restaurant in Janesville, Wisconsin.

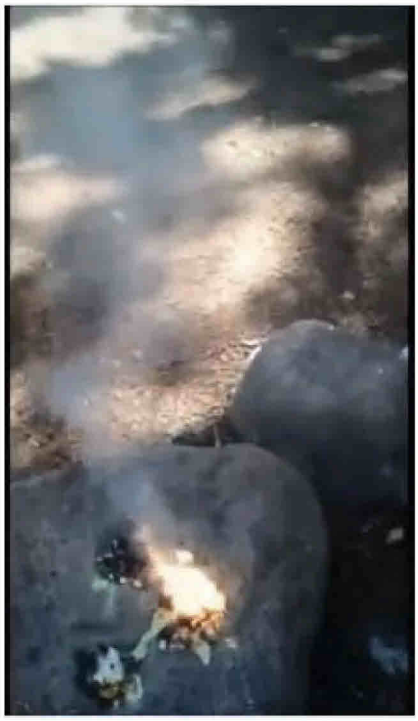
12. Open-source searches revealed social media accounts linked to Blome, including a YouTube channel, Facebook accounts, and an Instagram account. Legal process confirmed that Blome was associated with these accounts, as well as Google email accounts and an account at Gab.com, an internet communication platform.

13. On July 7, 2023, Magistrate Judge Nancy Joseph issued search warrants to Google LLC and Gab.com, which were executed on the same day. In response to the search warrants, Google LLC provided photos and videos created by Morgan and Gab.com provided direct message content.

## I. Choking Agent and Chlorine Gas

14. Blome has posted on social media information about how to create, and has demonstrated the use of, a smoke powder or choking agent. On August 9, 2019, Blome posted a video on Facebook titled, "Blome Waffenkreationen – BWk," which translates from German as "Weapon Creations." In the video, Blome provided the ingredients to create sulfur dioxide/trioxide smoke powder and demonstrated the use of setting a chemical mixture aflame to create a smoke cloud. After stepping into the cloud to test the effects, he stated, "huge smoke cloud of a choking agent," and "looks like I'm on the road to success then after all." Additionally, he provided clarifying instructions for the construction of the device.



15. On August 30, 2019, Blome published a YouTube video titled, "BWk- Sulfur X-Oxide Grenade Prototype Test." Blome demonstrated the use of the homemade chemical choking agent stating, "well that was a total success." At the end of the video text states, "production to begin when I have funds."

16. On October 6, 2019, Blome posted to Facebook, "Everyone . . . I'm forming my own militia. We will be called . . . The New American Minutemen. We stand for freedom. Plain and Simple. We are decentralized. I created it, but it does not belong to me. . . . America has been losing their God given freedoms one by one. I intend to defend these. I am enraged. Our government taxes us endlessly, forces us to send our children to schools they control, control the press with their laws, and they've established over 700 imperialistic bases overseas and expect us to pay for them. . . . Seems like we need to dust off our guns and do this again, my fellow Americans. And if anything happens to me because I said this . . . well that should just prove our basic rights no longer exist. Who will answer this call to arms? Who's with me?"

17. An anonymous tip provided to the FBI in November 2019 by a Facebook friend of Blome claimed Blome posted a video on Facebook depicting how to produce an acid gun to shoot sulfuric acid and stated in the video "governments should be afraid of their people. So here's how you make a device that shoots sulfuric acid!"

18. Blome contacted the Wisconsin Department of Justice (DOJ) on November 5, 2019, after being notified by his father that the Wisconsin DOJ and the Janesville Police Department

unsuccessfully attempted to contact Blome. During the interview, Blome admitted making several homemade weapons to protect himself before abruptly ending the phone call.

19. On November 28, 2019, Blome posted on Facebook about an encounter he had with law enforcement regarding "weapons I invented." He stated, "I was a chemistry major in college . . . I know what I'm doing," "any gun I do ever have will be undocumented," and "Like I even really need a conventional weapon? I'm a weapon designer mf! I can likely invent something better anyway."

20. On March 20, 2020, Blome recorded a video (saved to Google Photos) displaying the chemicals calcium hypochlorite and hydrochloric acid. When shown, Blome stated the chemicals were for making, "a lot of chlorine very quickly." Chorine gas is a pulmonary irritant and was first used as a chemical weapon during World War I by the Germans in 1915.

21. On March 10, 2020, Blome took a picture of the same chemicals.


22. On October 16, 2021, Blome took a photo of the same chemicals in addition to other chemicals used for making destructive devices and chemical weapons.


23. On July 8, 2022, Blome visited the following webpages entitled:

a. Calcium Hypochlorite 99% PURE MIN. (70% Chlorine Min.) 1lb Bottle | eBay;

b. Buy CCS LLC Hydrochloric Acid 37% High Purity 32oz (1000ml) - on sale today;

c. 37 hydrochloric acid 1 liter - Google Search;

d. Hydrochloric Acid 37% Reagent Grade for High Purity Aqua Regia (Pint): Amazon.com: Industrial & Scientific;

e. Buy Hydrochloric Acid 37% Solution, ACS Reagent Grade 30ml $24 For Sale Online; and

f. Amazon.com : 37% Hydrochloric acid.

24. On July 28, 2022, Blome took a photo of the chemistry equipment setup in his apartment.

25. During an interview of Fox Meadows Apartment employees in November 2023, the maintenance technician stated that, when in the apartment to change a smoke detector in the spring of 2023, he observed chemistry equipment set up in the bedroom of Morgan's apartment.

26. On May 10, 2023, Morgan sent the following direct messages on Gab to user @wisteria_frost regarding the creation and use of chlorine gas against an anticipated group of twenty government agents:

a. [2023-05-10 20:42:30 UTC] <RealJM1993> Or if it's goobermint coming for the guns...I have a different plan entirely. We'll defeat them without firing a single shot.

b. [2023-05-10 20:43:42 UTC] <Wisteria_Frost> Yeah, the 9mm or shotty, got it, hun. Of course, darling.

c. [2023-05-10 20:45:48 UTC] <RealJM1993> If it's goobermint coming for the guns...-throws you a gas mask- Get it on NOW! -reacts calcium hypochlorite with hydrochloric acid, producing a huge amount of chlorine in the confined space of the apartment-...now watch. Goobermint like a bunch of retards is gonna do their fave strategy where 20 guys charge in all at once.

d. [2023-05-10 20:47:22 UTC] <Wisteria_Frost> Of course, I'll follow your plan if we have to deal with them, darling.

e. [2023-05-10 20:49:00 UTC] <RealJM1993> Do you like that plan?

f. [2023-05-10 20:51:01 UTC] <Wisteria_Frost> Yes, I love your plan. You're awesome when it comes to planning stuff.

g. [2023-05-10 20:53:45 UTC] <RealJM1993> Then once they haven't heard from or seen their strike team for a good minute, they're gonna be really scared. Lol

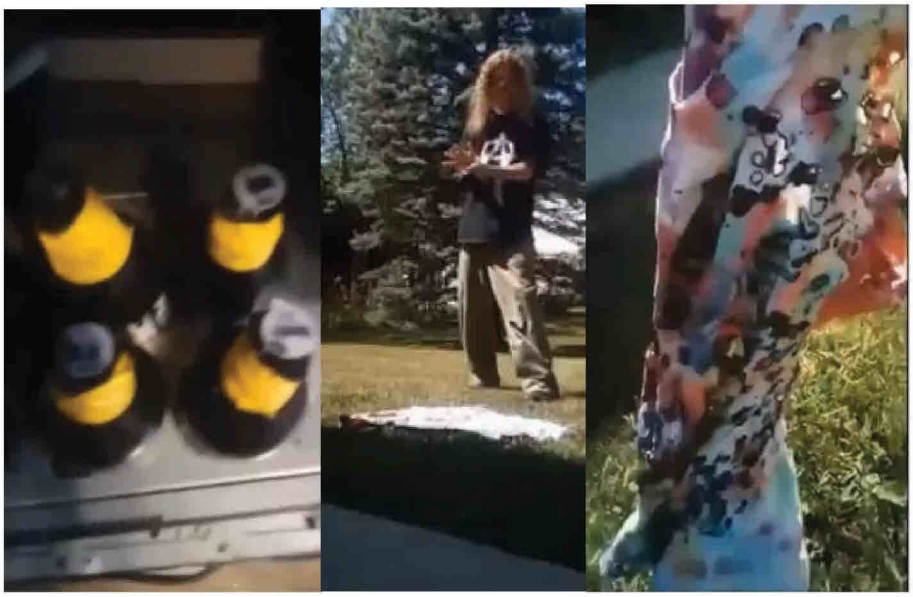
## II. Acid Sprayer

27. Blome has also posted information about how to create, and demonstrated the use of, a device to spray sulfuric acid. Records provided from Duda Energy (www.dudadiesel.com) revealed that on July 15, 2019, Blome purchased two 950mL quantities of 98% concentration sulfuric acid.

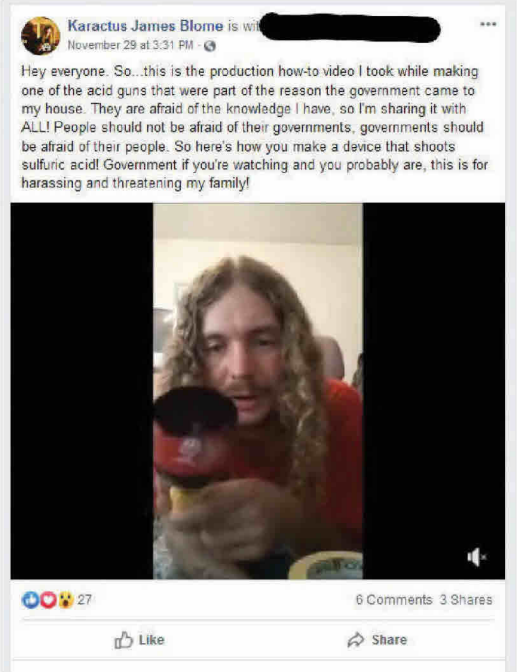
28. On August 28, 2019, Blome recorded a video titled, "acidthrowerinfomercial" where he stated that he was creating an acid sprayer in response to being threatened by Antifa. During the video, Blome showed how to use the acid sprayer and its burning effects on clothing, and stated, "chemically burn commies alive and melt their faces off for $10" and "message me on Facebook to take advantage of this amazing deal."

29. On August 31, 2019, Blome posted a YouTube video titled, "BWk – XW-M2 Saurewerfer," (which translates from German as "Acid Thrower"). In the video, Blome showed multiple premade XW-M2 acid throwers and demonstrated how to use them to fire sulfuric acid. Later in the video he demonstrated how the sulfuric acid damages concrete and burns through clothing. The

end of the video said, "Available for $10, acid not included. Sulfuric acid can be purchased at http://www.dudadiesel.com."



30. On November 29, 2019, Blome posted on Facebook a video about how to create and use a device to spray sulfuric acid. When posting the video Blome stated, "this is the production how-to video I took while making one of the acid guns that were part of the reason the government came to my house" and "People should not be afraid of their government, governments should be afraid of their people. So here's how you make a device that shoots sulfuric acid!"




31. On December 4, 2019, Blome posted a video on YouTube titled, "How to make a gun that shoots sulfuric acid." In the video Blome demonstrated how to create a device to spray sulfuric acid. He provided the name of "XWM2 Acid Thrower" or "Experimentalwaffe Modell Zwei Saurewerfer," which translates from German as "Experimental Weapon Model Two Acid Throwers." He stated the purpose is to shoot 98% pure sulfuric acid stating, "yeah, nasty stuff." He used black sealant and yellow tape to construct the device, stating that the color scheme was intentional like a bee or wasp to warn someone, "that I'm about to shoot something really nasty at you." He then demonstrated in the video how to fire the device and showed the damage the acid caused to concrete.

32. On March 16, 2020, Blome recorded a video (saved to Google Photos) where he described using a glass syringe to create an acid sprayer that was breech loaded, i.e., that could be refilled and fired multiple times in a short period of time.


33. On January 12, 2023, the FBI Scientific Response and Analysis Unit provided an analysis of the acid thrower weapon. The report provided the chemical reactions depicted in the video are consistent with concentrated sulfuric acid. Additionally, the report provided that attacks involving acids are known to cause disfiguring skin injuries and blindness if splashed into the eyes.

**III. Destructive Devices, Firearms, and Other Weapons**

34. On January 19, 2020, Blome posted on Facebook, "I'm a loose cannon when I speak and I really don't have that much space between thought and action. Consequences often don't even register in my mind when I get heated, I just act."

35. In February and March 2020, Blome's Facebook friend (discussed above in paragraph 17) provided additional information to the FBI about Blome sending private Facebook messages stating he disliked the police and claiming he would be going after law enforcement and the government.

36. On March 20, 2020, Blome recorded a video showing the supplies necessary to create homemade destructive devices. In the video, Blome states, "for making the things that go boom."


37. Purchase records provided by Classic Firearms of Indian Trail, North Carolina, revealed that on April 15, 2020, Blome purchased a Zastava Arms 7.62x39mm caliber AK-47 and had it shipped to CTR Firearms LLC in Janesville, Wisconsin.

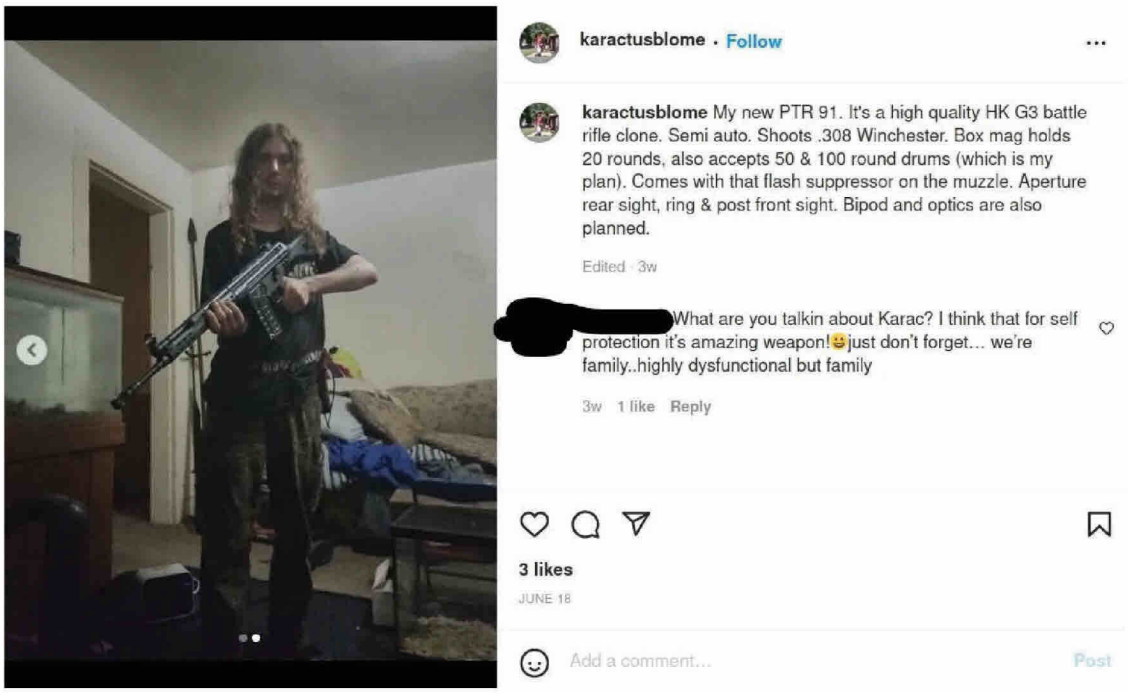
38. On April 19, 2022, Blome took a picture of the supplies necessary for making destructive devices including smokeless powder, cardboard containers, hobby fuse, glue, and nails.


39. On May 18, 2022, Blome posted a video on Instagram under display name "karactusblome" with the location set as Janesville, Wisconsin, displaying multiple firearms and

ammunition including two bolt action rifles, a semi-automatic rifle, a .44 caliber revolver, 7.5mm x 55mm ammunition, and multiple high-capacity drum ammunition magazines.

40. Purchase records provided from Atlantic Firearms in Bishop, Maryland, revealed that on June 10, 2022, Blome purchased a PTR-91 A3S .308 caliber rifle and had it shipped to CTR Firearms LLC in Janesville, Wisconsin.

41. On June 18, 2022, Blome posted on Instagram under display name "karactusblome" an image of himself holding a PTR-91 semi-automatic rifle.



42. On June 29, 2022, Blome posted on Instagram under display name "karactusblome" an image of a PTR-91 .308 caliber semi-automatic rifle and two high-capacity drum magazines.


43. On July 1, 2022, Blome posted on Instagram under display name "karactusblome" a video displaying multiple firearms in his bedroom including a PTR 91 semi-automatic rifle with multiple drum magazines of ammunition, a .44 caliber revolver, and ammunition.

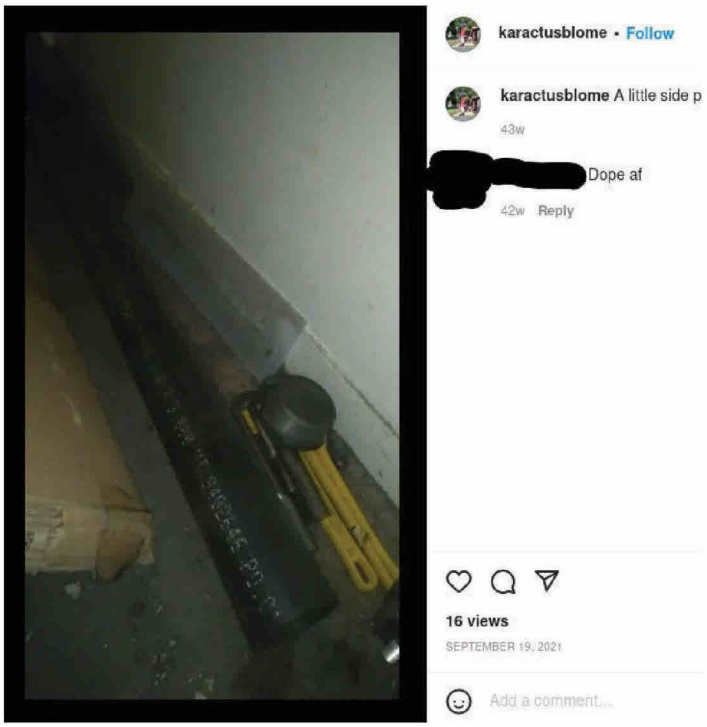
44. Financial records provided during the investigation revealed multiple firearms purchases by Blome from April 15, 2020, through June 10, 2022, totaling $2,813.32. Additionally, financial records revealed a total of $1,250 of expenditures from November 27, 2020, through July 2, 2022, at firearms and sporting goods stores for ammunition and firearms accessories.

45. On October 6, 2022, Blome posted a video on YouTube titled, "Bean-Delete bison Chili." At 0:37 in the video, the book titled, "Anarchist Cookbook" is observed on the table. The Anarchist Cookbook contains various instructions on how to create and manufacture improvised weapons and explosives.

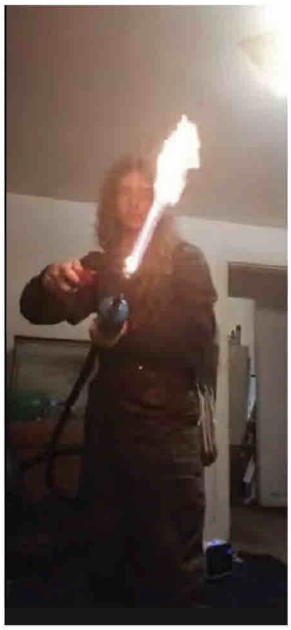

46. Blome has also revealed an intention to build and sell firearms, specifically a cannon-style weapon. On February 18, 2021, Blome posted on Gab:

> Hello folks. I noticed that the civilian arsenal is lacking in artillery due primarily to its cost and I want to fix this. So I'm starting a company whose mission is to make artillery affordable to the common man. My proposed design for a 7.62cm field gun would only cost around $1500 . . . about the same price as your typical AR15. It's a breech loader with a screw breech. The planned carriage is to be made of oak. The law is a little funny with artillery. Artillery cannot use "fixed cartridges" and artillery shells are "destructive devices." Solely to get around this and for no other reason, my artillery pieces will use paper cartridges. In order to get this started, I need a workshop and machinery so I am looking for investors. If affordable artillery is something you'd like to see, let's talk.

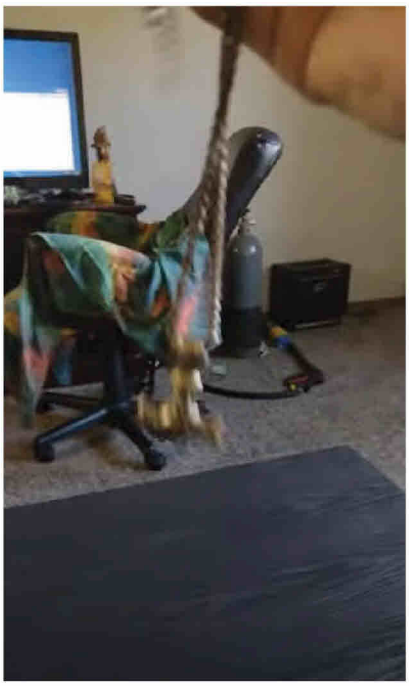
47. On September 19, 2021, Blome posted on Instagram a video explaining his plan to build his own 7.62cm (3 inch) "cannon" using a large pipe, threaded breech plug, and ball projectiles. In the video, Blome stated, "I was planning to mass produce them" for about $1,000 to $1,500 each, making "artillery available to the common man" and "yes, I do intend to finish this project." Blome did not register any such destructive devices under the National Firearms Act.




48. Blome has also revealed an intention to build a flamethrower. On May 12, 2022, Blome posted on YouTube a video titled, "Finishing up my Flamethrower." In the video he showed the components and design to create a gasoline flamethrower.



49. On August 26, 2022, Blome posted on YouTube a video titled, "My Daily Workout." At 5:10 in the video, the above flamethrower is in the background of what appears to be Blome's apartment in Whitewater, Wisconsin.



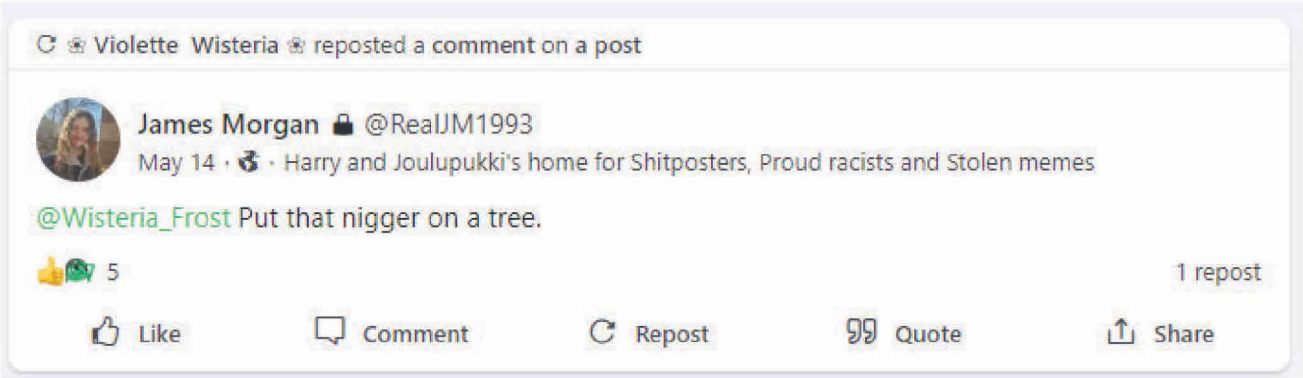
50. In May 2023, a co-worker of Morgan's (formerly known as Blome) at Generac stated that Morgan said he learned how to make bombs at school. Another co-worker stated that they were concerned Morgan would be "the first person to go postal."

51. In May 2023, Morgan was interviewed by the FBI and Whitewater Police Department in relation to a reported missing person welfare check of an individual, C.L., that was requested by Seabrook New Hampshire Police Department. During the interview, Morgan stated C.L. was his girlfriend and they met on the social media platform, Gab.com.

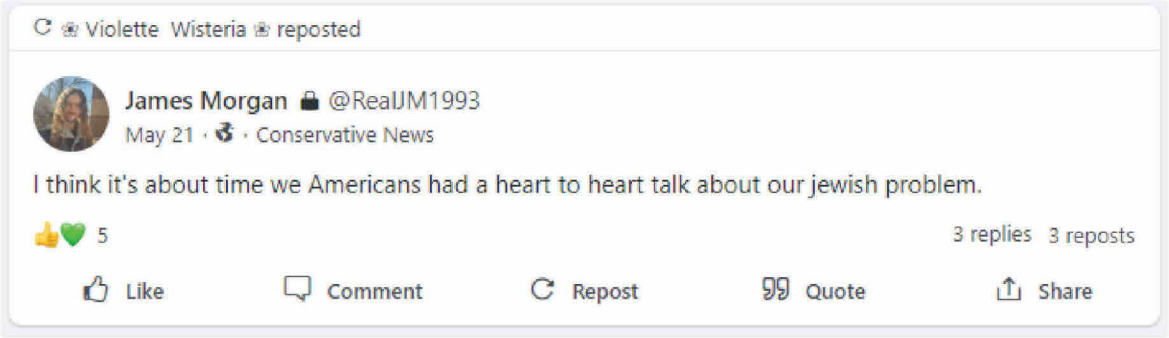
52. Records provided from Gab.com during the investigation revealed James Morgan as the subscriber for username @RealJM1993 (display name James Morgan) created January 21, 2021. Morgan stated in the "about" section of the profile that he was in a relationship with @Wisteria_Frost

(display name Violette Wisteria). Open-source review of Gab.com revealed that @RealJM1993 is a private account but has some posts that are viewable publicly because they were reposted by user @Wisteria_Frost, including the following posts:

a. On May 14, 2023, user @RealJM1993 (James Morgan) posted in response to a screenshot of a Reddit post showing a white teacher being asked to show respect by kissing a black student's hand:

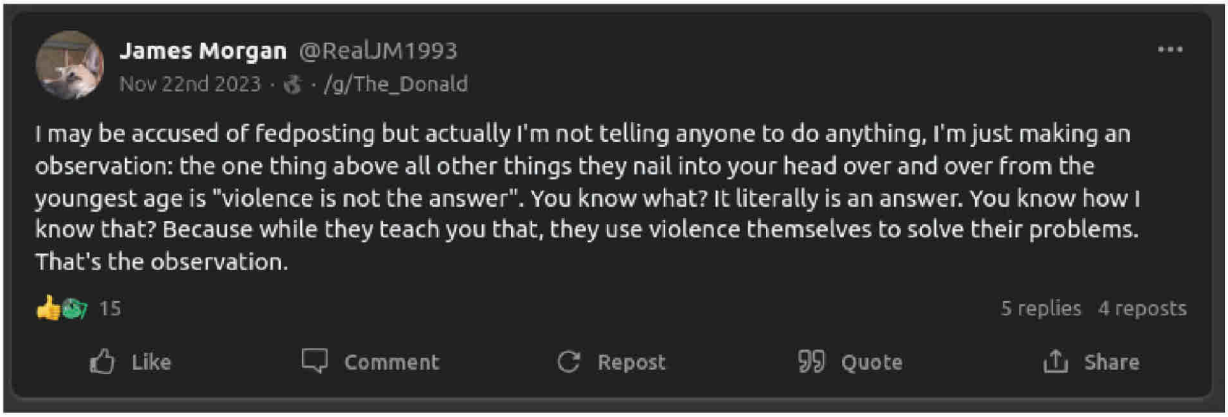



b. On May 21, 2023, Morgan posted:




c. On May 29, 2023, Morgan posted:

d. On November 22, 2023, Morgan posted:




53. On December 7, 2023, @Wisteria_Frost (display name Violette Wisteria) posted: "All cops can die. I fucking hate cops as much as I hate niggers. The only good cop is a dead cop."

54. A review of Blome's Google account after the July 2023 search warrant revealed an 80-page Adobe Acrobat document entitled, Home Expedient Firearms-9mm SMG.pdf, a digital book of instructions on how to make a homemade submachine gun.

## IV. Current Residence, Vehicle, and Storage Unit

55. Blome has for several years engaged in a continuing pattern of activity, using chemicals and constructing devices for use as weapons. He has engaged in this activity at his prior residences in Janesville (beginning in August 2019) and Whitewater, Wisconsin (beginning in June 2022). He has made statements regarding the use of such weapons against government agents, specifically law enforcement, and statements regarding violence against people of different races.

56. On June 12, 2023, FBI physical surveillance observed Morgan tell the Fox Meadows apartment complex office he would "be out by July 31" of the Fox Meadows apartments, located at 291 N. Fraternity Lane, Whitewater, Wisconsin.

57. On November 28, 2023, employees of the Fox Meadows Apartment complex provided information that Morgan's lease at Fox Meadows Apartments was from July 1, 2022, through July 31,

2023. His lease was not renewed by the management due to concerns about the poor condition of the unit, as well as concerns about Morgan's possession of a homemade flamethrower and unsecured firearms, and his open carrying of a handgun.

58. According to the Fox Meadows employees, Morgan moved all his belongings from his apartment into a travel trailer in the apartment complex's parking lot. Morgan temporarily lived in the trailer in that parking lot until management required that the trailer be moved. An employee of the apartment complex later saw Morgan's blue pickup and trailer parked at the Whitewater bowling alley parking lot in early- to mid-November 2023.

59. In or about early August 2023, Morgan moved his belongings from his apartment at Fox Meadows to a white 2014 Forest River Grey Wolf travel trailer bearing Illinois license plate 800938RT. Public databases revealed that an ID66 camper trailer bearing that license plate number and Vehicle Identification Number (VIN): 4X4TCKB28EK023093, was registered to Morgan's mother on August 9, 2023, with an address in Wheeling, Illinois. Morgan is not believed to have another residence currently. On December 5, 2023, Morgan posted on Gab about the solar panels in the bed of his truck, indicating an intent to reside in the trailer for an extended time.

60. As of June 12, 2023, FBI physical surveillance observed a white Honda Accord bearing Wisconsin license plate AJN9507 and black Ford Ranger bearing Wisconsin license plate TF4493 (both registered to James Morgan) located in the parking lot of the Fox Meadow Apartments.

61. Morgan traded in the Ford Ranger at Berger Motors for a blue 2000 Dodge Ram 1500, which public databases revealed was registered to James Morgan on September 26, 2023, bearing Wisconsin license plate TF4493, VIN: 1B7HF16Z0YS539750, and a mailing address of Post Office Box 624, Whitewater, Wisconsin (Walworth County).

62. Physical surveillance conducted by the FBI observed the trailer connected to a blue 2000 Dodge Ram 1500 bearing Wisconsin license plate TF4493 at the following locations:

a. August 7, 2023 – Walmart, 3800 Deerfield Dr., Janesville, WI (Rock County);
b. August 9, 2023 – Spacesaver, 1700 Janesville, Rd., Fort Atkinson, WI (Jefferson County);
c. August 16 through 21, 2023 – Pilgrims Campground, W7271 County Rd. C, Fort Atkinson, WI (Jefferson County);
d. September 20, 2023 – Hawk Apartments, 1380 W Main St., Whitewater, WI (Walworth County);
e. October 23, 2023 – The Marketplace, 2799 Pontiac Place, Janesville, WI (Rock County);
f. December 5, 2023 – The Marketplace, 2799 Pontiac Place, Janesville, WI (Rock County); and
g. December 12, 2023 – The Marketplace, 2799 Pontiac Place, Janesville, WI (Rock County).

63. On November 18, 2022, Whitewater Self Storage provided information that Karactus Blome was renting unit #114 at W8290 Sunrise Ln, Whitewater, WI. Whitewater Self Storage provided information that James Morgan was current on payments for unit #114 as of October 26, 2023.

64. Based on my training and experience, I know that persons engaged in illegal activities, such as the possession of chemical weapons, teaching or demonstrating the making or use of weapons of mass destruction, conspiracy, threats, and possessing or making firearms and destructive devices in violation of the National Firearms Act, commonly store records of and components used to make such weapons and destructive devices at their residences and in their storage units.

65. Based on my training and experience, I know that individuals use mobile telephones and other electronic devices such as tablets and computers to connect to the Internet and to communicate using various messaging applications, including to make or coordinate travel plans and meetings with associates and to communicate with others before, during, or after, criminal activity. Information provided in response to legal process indicated that Morgan has used a Motorola Moto G Power, IMEI 35689111307451. Phones and devices can store communications, text messages, text files/notes, and

application data (including encrypted chat applications) that can show planning, preparation, and execution of the subject offenses.

66. Based on my training and experience, I know cellular telephone users typically keep those devices on their person or within close proximity to their person at most times of day and night. Based on my training and experience, I know that individuals can change the make and model of their cell phone while retaining the same phone number. I further know that many cell phones have the capability for users to personalize their devices, including installing and using applications such as Facebook, Google, and other services, and that a user can access their own account(s) from different devices.

67. Based on my training and experience, I also know that when cellular telephone users are driving a vehicle, they frequently place their cellular telephones within the passenger compartment of the vehicle so they are more readily accessible to make and receive phone calls or messages, to use navigation features, or to interact with a variety of other mobile applications. I also know based on my training and experience that individuals store clothing, accessories, and other items in their vehicles.

68. Based on my knowledge, training, and experience, I know evidence of fraud is often stored and transmitted via mobile telephones and electronic devices such as computers, memory cards, and flash drives. Additionally, electronic files are often transferred from one device to another via cloud computing storage services such as Apple iCloud, Google Drive, Sync, and Dropbox.

## COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

69. As described above and in Attachment B, this application seeks permission to search for records that might be found at the residence, vehicle, or storage unit of Morgan's, or on or near Morgan's person, in whatever form they might be found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, to include laptops and cellular

telephones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

70. "Digital device," as used herein, includes the following three terms and their respective definitions:

a. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

b. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

c. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy

disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

e. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap"

protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage,

and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

k. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

l. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

m. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should

not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

n. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

71. *Probable Cause.* I submit that if a computer or storage medium (including a cellular telephone) is found at the residence, vehicle, or storage unit of Morgan's, or on or near Morgan's person, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. In addition, in my training and experience, I know it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offenses under investigation that originally resided on one digital device belonging to Morgan may also be saved to other digital devices belonging to him. Based on that, there is also probable cause to believe that evidence related to these offenses may have

been transferred to and stored on digital devices beyond the particular digital device Morgan possessed during the commission of the offenses. For example, computers or other storage media may contain evidence of the subject offenses or planning and preparation for Morgan's activities.

72. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, location information, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may

provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

73. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of the three premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be

unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

74. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a storage medium to human inspection in order to determine whether it is evidence described by the warrant.

**BIOMETRIC ACCESS TO DEVICE(S)**

75. This warrant permits law enforcement agents to obtain from the person of Morgan (but not any other individuals at the time of execution of the warrants) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is

found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced

by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours

has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the residence, vehicles, or storage unit of Morgan's, or on or near Morgan's person,; (2) hold such Device(s) found in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold such Device(s) in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

i. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify

specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

## CONCLUSION

76. Based on the information and facts above, I submit that this affidavit supports probable cause to search the items described in Attachment A and seize the items described in Attachment B.

**ATTACHMENT A**

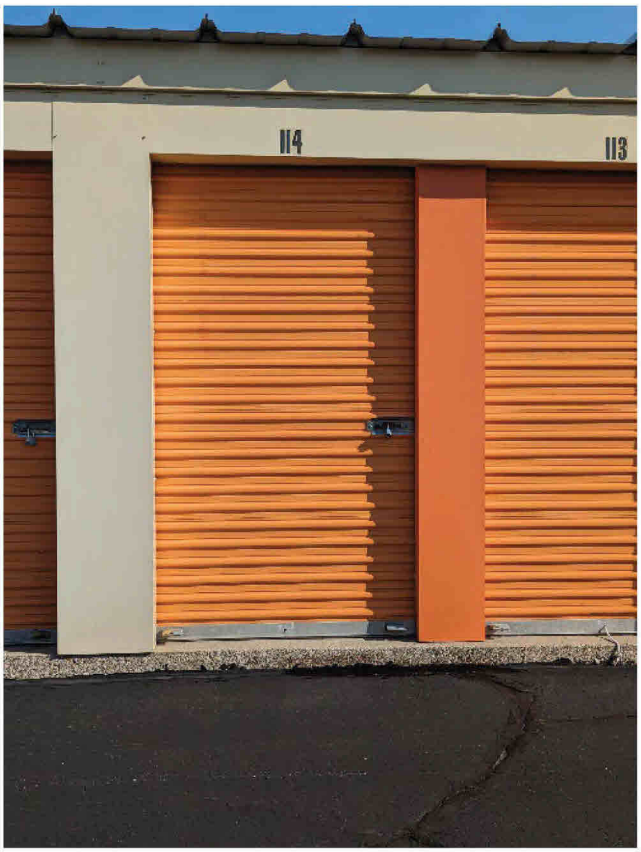
**Property and Person to Be Searched**

The property and person to be searched are:

– White 2014 Forest River Grey Wolf travel trailer bearing Illinois license plate 800938RT, VIN: 4X4TCKB28EK023093, that is the residence of James Morgan (formerly known as Karactus Blome).


– Blue 2000 Dodge Ram 1500 bearing Wisconsin license plate TF4493, VIN 1B7HF16Z0YS539750.


– Whitewater Self Storage Unit #114, W8290 Sunrise Ln, Whitewater, Wisconsin. The storage unit is a locked unit with the unit number located directly above the door.




– The person of James Morgan (formerly Karactus Blome) (DOB: 5/9/1993, including all items in his possession, on his person, or in areas within his immediate control.

# ATTACHMENT B

## Particular Things to be Seized

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 842(p) (teaching or demonstrating the making or use of weapons of mass destruction), 18 U.S.C. § 229(a) (develop, produce, possess or conspire to use a chemical weapon), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 875(c) (communication of threats), and 26 U.S.C. § 5861 (receive, possess, or make firearm or destructive device in violation of the National Firearms Act) (the "subject offenses") involving James Morgan (aka Karactus Blome) and occurring after August 1, 2019, including:

1. Records and information relating to the subject offenses described above, including chemical weapons, chemical weapon precursor chemicals, weapons of mass destruction, and destructive devices;

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the subject offenses;

3. Preparatory steps taken in furtherance of those offenses;

4. Evidence of motive, intent, or knowledge of those offenses;

5. Computers or storage media that constitute fruits, contraband, evidence, or instrumentalities of the crimes described in the warrant.

6. For any storage medium whose seizure is otherwise authorized by this warrant, and any storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "computer"):

a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

h. evidence of the times the computer was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the computer;

j. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

k. records of or information about Internet Protocol addresses used by the computer;

l. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, cell phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files, web cache information, and handwritten notes), regarding the subject offenses.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. During the execution of the search of the premises described in Attachment A, law enforcement personnel are also specifically authorized to compel James Morgan (formerly known as Karactus Blome) to provide biometric features, including pressing fingers (including thumbs) against and or putting a face before a sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the premises, and
b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the subject offenses as described in the search warrant affidavit and warrant attachments

for the purpose of attempting to unlock the device's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to request Morgan state or otherwise provide the passcode or password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique fingers or other physical features) that may be used to unlock or access the devices.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.